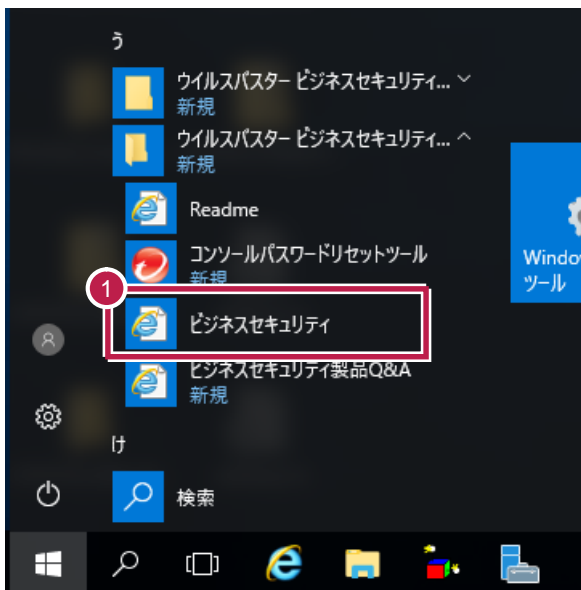


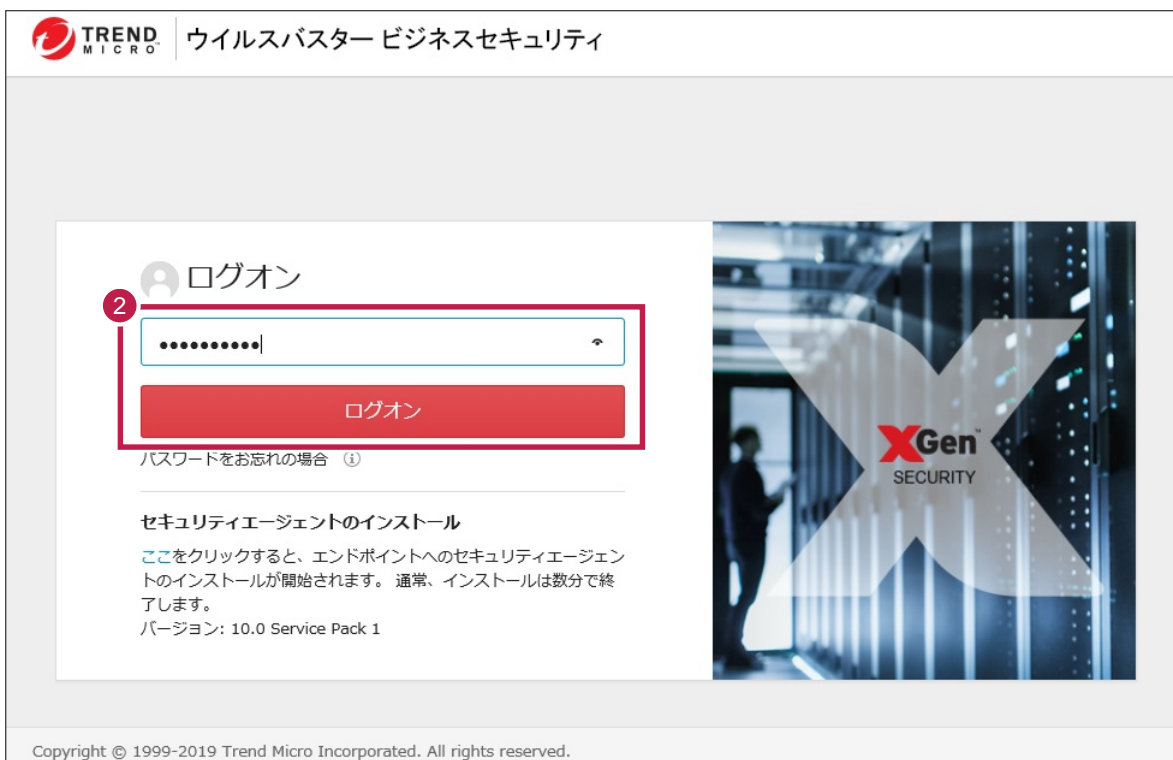
ウイルスバスター ビジネスセキュリティ Ver10 (サーバーの除外設定)

- 1 Windowsスタートメニューから [ビジネスセキュリティ] をクリックします。

【スタートメニュー】



- 2 管理者の方がパスワードを入力して、[ログオン] をクリックします。



リアルタイム検索の除外設定

- 1 [デバイス] をクリックします。

ウイルスバスター ビジネスセキュリティ

最新ステータス **デバイス** 検索 ▾ アップデート ▾ レポート ▾ 管理 ▾ ヘルプ ▾ ログオフ

前回のアップデート: 2019/12/4 11:18:37

処理は必要ありません。お使いのデバイスは保護されています。

セキュリティリスクの検出数 過去30日間 ▾

0 既知の脅威 0 未知の脅威 0 ポリシー違反

イベントの種類	影響を受けたデバイス	検出した脅威
ウイルス/不正プログラム	0	0
スパイウェア/グレーウェア	0	0
Webレピュテーション	0	0
ネットワークウイルス	0	0

ランサムウェアの概要 過去30日間 ▾ エージェントのステータス

- 2 左側のツリーから、除外設定するコンピュータグループを選択して [ポリシーの設定] をクリックします。

ウイルスバスター ビジネスセキュリティ

最新ステータス デバイス 検索 ▾ アップデート ▾ レポート ▾ 管理 ▾ ヘルプ ▾ ログオフ

デバイス 前回のアップデート

グループの追加

デスクトップ (初期設定) (1デバイス) 検索

+ デバイスの追加 **ポリシーの設定** 検索 ▾ ... 詳細 ▾

名前	スマートスキャンサービス	IPアドレス	ステータス	通常検索	アク
TESTPC20	接続		オンライン	該当なし	該当

3 [ウィルス/スパイウェア対策] をクリックします。

The screenshot shows the 'ウイルスバスター ビジネスセキュリティ' (Virus Buster Business Security) interface. The left sidebar contains a menu with '不正プログラム対策' (Malware Protection) expanded. Under it, '検索方法' (Search Method) is highlighted with a red box and a circled '3'. The main content area shows the '検索方法' (Search Method) settings. It includes a description of '従来型スキャン' (Legacy Scan) and 'スマートスキャン' (Smart Scan). The 'スマートスキャン' (Smart Scan) option is selected with a radio button and a circled '4'. A blue '保存' (Save) button is visible below the options.

4 [検索対象] タブの [検索除外] の [+] をクリックします。

The screenshot shows the 'ウイルスバスター ビジネスセキュリティ' (Virus Buster Business Security) interface. The left sidebar contains a menu with '不正プログラム対策' (Malware Protection) expanded. Under it, '検索方法' (Search Method) is expanded, and 'ウイルス/スパイウェア対策' (Virus/Spamware Protection) is highlighted with a red box and a circled '4'. The main content area shows the 'ウイルス/スパイウェア対策' (Virus/Spamware Protection) settings. It includes a toggle for 'リアルタイムのウイルス/スパイウェア対策を有効にする' (Enable real-time virus/spamware protection) which is turned on. Below it, the '検索対象' (Search Targets) tab is highlighted with a red box and a circled '4'. The '検索方法' (Search Method) section shows three radio button options: '検索可能なすべてのファイル' (All searchable files), 'トレンドマイクロの推奨設定: 実際のファイルタイプによる識別' (Trend Micro's recommended setting: Identification by actual file type), and '検索対象の拡張子の選択 (拡張子はそれぞれカンマで区切ってください)' (Select search target file extensions (separate each extension with a comma)). The second option is selected. Below this is a list of file extensions: ".*", ".ACCDB", ".ARJ", ".BAT", ".BIN", ".BOO", ".CAB", ".CHM", ".CLA", ".CLASS", ".COM", ".CSC", ".DLL", ".DOC", ".DOCM", ".DOCX", ".DOT", ".DOTM", ".DOTX", ".DRV", ".EML", ".EXE", ".GZ", ".HLP", ".HTA", ".HTM", ".HTML", ".HTT", ".INI", ".JAR", ".JPEG", ".JPG", ".JS", ".JSE", ".LNK", ".LZH", ".MDB", ".MPD", ".MPP", ".MPT", ".MSG", ".MSO", ".NWS", ".OCX", ".OFT", ".OVL", ".PDF", ".PHP", ".PIF", ".PL", ".POT", ".POTM", ".POTX", ".PPAM", ".PPS", ".PPSM", ".PPSX", ".PPT", ".PPTM", ".PPTX", ".PRC", ".". Below this is the '検索の実行方法' (Search execution method) section with three radio button options: '読み取り' (Read), '書き込み' (Write), and '読み取りまたは書き込み' (Read or write), which is selected. At the bottom, the '検索除外' (Exclude from search) button is highlighted with a red box and a circled '4'.

5 [検索除外を有効にする] がONであることを確認します。

6 弊社製品がインストールされているフォルダパス「C:¥FCAPP」を入力します。
(Cは弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。)
参照ツリーなどは表示されないの、手入力する必要があります。
指定したフォルダのサブフォルダも除外対象となります。

7 [追加] ボタンをクリックします。

The screenshot shows the 'ウイルスバスター ビジネスセキュリティ' (Virus Buster Business Security) interface. The left sidebar contains navigation options like '不正プログラム対策' (Malware Protection), 'ウイルススバイウェア対策' (Virus Protection), and 'WEB評価' (Web Evaluation). The main area is titled 'デバイス > ポリシーの設定: デスクトップ (初期設定)'. Under the '検索除外' (Search Exclusion) section, the checkbox '検索除外を有効にする' (Enable search exclusion) is checked and highlighted with a red box and the number 5. Below it, the '特定ディレクトリの検索除外' (Exclude specific directories) section is active. A text input field contains 'C:¥FCAPP', highlighted with a red box and the number 6. To the right of the input field is a red '追加' (Add) button, also highlighted with a red box and the number 7. There is also a '削除' (Delete) button below it.

8 下部のリストに、フォルダパスが追加されたことを確認します。

This screenshot shows the same interface as the previous one, but now the folder path 'C:¥FCAPP' has been added to the list of excluded directories. The '検索除外' (Search Exclusion) section is still active. The '特定ディレクトリの検索除外' (Exclude specific directories) section now shows a list with 'C:¥FCAPP' entered, highlighted with a red box and the number 8. The '追加' (Add) button is no longer visible, and the '削除' (Delete) button is now visible next to the entry in the list.

9 以下のフォルダーが存在する場合は、同様な手順で、それぞれリストに追加してください。

存在しない場合は追加不要です。

- ・32 ビットOS の場合「C:¥Program Files ¥Common Files¥Fukui Computer Shared」
- ・64 ビットOS の場合「C:¥Program Files (x86)¥Common Files¥Fukui Computer Shared」

トレンドマイクロ ウイルスバスター ビジネスセキュリティ

最新ステータス デバイス 検索 アップデート レポート 管理 ヘルプ ログオフ

デバイス > ポリシーの設定: デスクトップ (初期設定)

不正プログラム対策

検索方法

ウイルススバイウェア対策

機械学習型検索

挙動監視

信頼済みプログラム

隔離

WEB評価

Webレビューション

URLフィルタ

承認済み/ブロックするURL

その他の設定

ファイアウォール

デバイスコントロール

検索除外

検索除外を有効にする

特定ディレクトリの検索除外

トレンドマイクロ製品がインストールされているディレクトリを検索から除外する
ディレクトリのパスを入力してください (例: c:¥temp¥ExcludeDir。詳細については、製品Q&Aの事例を参照してください。)

追加

削除

C:¥FCAPP
C:¥Program Files (x86)¥Common Files¥Fukui Computer Shared

特定ファイルの検索除外

ファイル名またはファイルのフルパスを入力してください。
(例: ExcludeDoc.hlp; c:¥temp¥excldir¥ExcludeDoc.hlp。詳細については、製品Q&Aの事例を参照してください。)

10 追加が終わったら、下にスクロールして [保存] をクリックします。

トレンドマイクロ ウイルスバスター ビジネスセキュリティ

最新ステータス デバイス 検索 アップデート レポート 管理 ヘルプ ログオフ

デバイス > ポリシーの設定: デスクトップ (初期設定)

不正プログラム対策

検索方法

ウイルススバイウェア対策

機械学習型検索

挙動監視

信頼済みプログラム

隔離

WEB評価

Webレビューション

URLフィルタ

承認済み/ブロックするURL

その他の設定

ファイアウォール

デバイスコントロール

ユーザツール

エージェントの権限

特定の拡張子を持つファイルの検索除外

リストから拡張子を選択してください。

選択された拡張子:

XLSX
XLT
XLTM
XLTX
XML
Z
ZIP

追加

削除

EVT
EVTX
LOG
OST
PST

拡張子を入力してください。

詳細設定

保存

挙動監視の除外設定 / 信頼済みプログラムに追加

- 1 [挙動監視]、または [信頼済みプログラム] をクリックします。
ここでは [挙動監視] で記載しますが、 [信頼済みプログラム] も設定方法は同じです。
ただし、 [信頼済みプログラム] に有効化・無効化の設定はありません。

The screenshot shows the Trend Micro Virus Buster Business Security interface. The left sidebar is expanded to show the '挙動監視' (Behavior Monitoring) option, which is highlighted with a red box and a circled '1'. The main content area displays the '挙動監視' settings page, including a list of file extensions (XLSX, XLT, XLTM, XLTX, XML, Z, ZIP) and a '詳細設定' (Advanced Settings) section.

- 2 [挙動監視の有効化] がONであることを確認します。

The screenshot shows the Trend Micro Virus Buster Business Security interface. The left sidebar is expanded to show the '挙動監視' (Behavior Monitoring) option, which is highlighted with a red box and a circled '2'. The main content area displays the '挙動監視' settings page, including a toggle switch for '挙動監視の有効化' (Enable Behavior Monitoring) which is turned ON. Below the toggle, there are checkboxes for '不正プログラムの挙動ブロックを有効にする' (Enable behavior blocking of malicious programs) and 'HTTPまたはメールアプリケーションを介してダウンロードされた新しいプログラムを実行する前にユーザに確認する' (Confirm before running new programs downloaded via HTTP or email applications).

- 3 下にスクロールして [除外設定] のボックスに、「C:¥FCAPP」フォルダー内のexeファイルのパスを手入力します。
 例：C:¥FcApp¥EX-TREND武蔵¥Program¥FC.Fleet.Main.exe
 (Cは弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。)
 その他の除外設定するexeファイルは、P.9を参照してください。

- 4 [承認済みリストに追加] をクリックします。

ウイルスバスター ビジネスセキュリティ

デバイス > ポリシーの設定: デスクトップ (初期設定)

不正プログラム対策

検索方法

ウイルス/スパイウェア対策

機械学習型検索

挙動監視

信頼済みプログラム

隔離

WEB評価

Webレビュテーション

URLフィルタ

承認済み/ブロックするURL

その他の設定

ファイアウォール

デバイスコントロール

ユーザツール

除外設定

除外リスト内のプログラムは不審な挙動についての監視対象から除外されますが、ブロックリスト内のプログラムは自動的にブロックされます。

プログラムのフルパスを入力してください

例:C:¥Program Files¥BMDir¥BMSample.exe (複数指定する場合はセミコロンで区切ってください)

C:¥FcApp¥EX-TREND武蔵¥Program¥FC.Fleet.Main.exe

承認済みリストに追加

ブロックするリストに追加

承認済みプログラムリスト

名前	プログラムのフルパス

- 5 [承認済みプログラムリスト] に追加されたことを確認します。

ウイルスバスター ビジネスセキュリティ

デバイス > ポリシーの設定: デスクトップ (初期設定)

不正プログラム対策

検索方法

ウイルス/スパイウェア対策

機械学習型検索

挙動監視

信頼済みプログラム

隔離

WEB評価

Webレビュテーション

URLフィルタ

承認済み/ブロックするURL

その他の設定

ファイアウォール

デバイスコントロール

ユーザツール

除外設定

除外リスト内のプログラムは不審な挙動についての監視対象から除外されますが、ブロックリスト内のプログラムは自動的にブロックされます。

プログラムのフルパスを入力してください

例:C:¥Program Files¥BMDir¥BMSample.exe (複数指定する場合はセミコロンで区切ってください)

承認済みリストに追加

ブロックするリストに追加

承認済みプログラムリスト

名前	プログラムのフルパス
FC.Fleet.Main.exe	C:¥FcApp¥EX-TREND武蔵¥Program¥FC.Fleet.Main.exe

6 同様な手順で、必要なファイルをすべてリストに追加してください。

7 追加が終わったら、[保存] をクリックします。

最新ステータス デバイス 検索 アップデート レポート 管理 ヘルプ ログオフ

デバイス > ポリシーの設定: デスクトップ (初期設定)

不正プログラム対策

検索方法

ウイルス/スパイウェア対策

機械学習型検索

挙動監視

信頼済みプログラム

隔離

WEB評価

Webレピュテーション

URLフィルタ

承認済み/ブロックするURL

その他の設定

ファイアウォール

デバイスコントロール

ユーザツール

エージェントの権限

承認済みプログラムリスト

名前	プログラムのフルパス	
FC.Fleet.Main.exe	C:\FCAPP\EX-TREND武蔵\Program\FC.Fleet.Main.exe	×
FC.Procedure.Main.exe	C:\FCAPP\EX-TREND武蔵\Program\FC.Procedure.Main.exe	×

ブロックするプログラムリスト

名前	プログラムのフルパス	

保存

EX-TREND 武蔵に関して除外設定をおすすめする EXE ファイル一覧

(ウイルスとして誤認識された場合に、除外設定の参考にしてください。)

EX-TREND 武蔵			
No	EXE ファイルが存在するフォルダパス	EXE ファイル名	関係するプログラム
1	C:¥FCAPP¥EX-TREND 武蔵¥Program	FC.Fleet.Main.exe	インデックス
2		FC.Procedure.Main.exe	施工計画書作成支援
3		CCad.exe	建設 CAD
4		FC.Scheduler.exe	工程管理
5		FC.CsManager.exe	原価工程管理
6		ExPhoto.exe	写真管理
7		ExAlbum.exe	アルバム編集
8		ExDeki.exe	出来形管理
9		ExPave.exe	舗装出来形管理
10		ExQual.exe	アスファルト温度管理
11			コンクリート品質管理
12		TrndEnou.exe	電子納品ツール
13	C:¥FCAPP¥FCNCLCenter	FCNCLCenter.exe	ネット認証ライセンスセンター
14	C:¥FCAPP¥Concierge¥Program	TRENDLive.exe	FC コンシェルジュ

Cは弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。

弊社の他プログラムでも、ウイルスとして誤認識される場合があります。

その時は各プログラム (program) フォルダ内の誤認識された EXE ファイルを除外設定して下さい。

例)

- ・TREND-ONE の場合 「C:¥FCAPP¥TREND-ONE¥Program」フォルダ以下の EXE ファイル
- ・BTXA の場合 「C:¥FCAPP¥BTXA¥Program」フォルダ以下の EXE ファイル

ファイアウォールの除外設定

SNS - LANプロテクト、またはTREND-ONE、Mercury-ONE、BLUETREND XAの共同編集機能をご利用のお客様は [ファイアウォール] に除外設定をしてください。その他のお客様は設定の必要はありません。

1 [ファイアウォール] をクリックします。

The screenshot shows the Trend Micro Virus Buster Business Security web interface. The top navigation bar includes '最新ステータス', 'デバイス', '検索', 'アップデート', 'レポート', '管理', and 'ヘルプ'. The main content area is titled 'デバイス > ポリシーの設定: デスクトップ (初期設定)'. On the left sidebar, under 'その他の設定', the 'ファイアウォール' (Firewall) option is highlighted with a red box and a circled '1'. Below it are 'デバイスコントロール', 'ユーザツール', and 'エージェントの権限'. The main panel shows two empty tables for '名前' and 'プログラムのフルパス' under 'ブロックするプログラムリスト'. A '保存' (Save) button is visible at the bottom.

2 [オフィス内] の [ファイアウォールを有効にする] がONで、[詳細モード] であることを確認してください。

The screenshot shows the 'ファイアウォール - オフィス内' (Firewall - Office) settings page. The left sidebar has 'ファイアウォール' expanded, with 'オフィス内' (Office) selected and highlighted with a red box. The main panel contains the following information:

- ファイアウォール - オフィス内** (with a help icon):
 - ファイアウォールを無効にすると、ネットワークウイルス保護や大規模感染予防ポリシー (大規模感染予防) のポートブロックも無効になります。
 - [ロケーション認識] が無効にされている場合、[オフィス内] 設定は初期設定として動作します。
 - ロケーション認識の設定を確認してください。
- ファイアウォールを有効にする** (checked):
 - 簡単モード: トレンドマイクロの初期設定を使用
 - 詳細モード: セキュリティレベル、IDS、通知、および除外を設定
- セキュリティレベル**:
 - トラフィックのルールを選択してください (除外リストのポート以外に適用)。
 - 高: すべての送受信トラフィックがブロック (拒否) されます。
 - 中: 受信トラフィックがブロック (拒否) され、送信トラフィックが許可されます。
 - 低: すべての送受信トラフィックが許可されます。
- 設定**:
 - IDS (侵入検知システム) を有効にする
 - 警告メッセージを有効にする

3 下にスクロールして、[除外設定] の [追加] をクリックします。

不正プログラム対策

検索方法

ウイルス/スパイウェア対策

機械学習型検索

挙動監視

信頼済みプログラム

隔離

WEB評価

Webレピュテーション

URLフィルタ

承認済み/ブロックするURL

除外設定

除外設定を追加または編集します。

+ 追加

編集

削除

上に移動

下に移動

<input type="checkbox"/>	ID	名前	処理	方向	プロトコル	ポート/ポート範囲	コンピュータ
<input type="checkbox"/>	1	DNS	許可	送受信	TCP/UDP	指定: 53	すべて
<input type="checkbox"/>	2	NetBIOS	許可	送受信	TCP/UDP	指定: 137、...	すべて
<input type="checkbox"/>	3	HTTPS	許可	送受信	TCP	指定: 443	すべて
<input type="checkbox"/>	4	HTTP	許可	送受信	TCP	指定: 80	すべて
<input type="checkbox"/>	5	Telnet	許可	送受信	TCP	指定: 23	すべて
<input type="checkbox"/>	6	SMTP	許可	送受信	TCP	指定: 25	すべて

4 下表に従って設定します。画像は、「SNS - LAN」の設定内容になっています。

名前	処理	方向	プロトコル	ポート	コンピュータ
SNS - LAN	許可	送受信	UDP	指定 : 5093	すべての IP アドレス
SQL Server Express	許可	受信	TCP	指定 : 1435	すべての IP アドレス
SQL Browser	許可	受信	UDP	指定 : 1434	すべての IP アドレス
MTS	許可	送受信	TCP	指定 : 8103	すべての IP アドレス

ファイアウォール設定 > 除外設定の追加/編集

名前: SNS-LAN

処理: ネットワークトラフィックを許可

方向: 受信 送信

プロトコル: UDP

ポート: すべてのポート 範囲: 開始値 終了値 指定ポート: 5093

コンピュータ: すべてのIPアドレス 単一IP

ホスト名:

5 下にスクロールして、[保存] をクリックします。

ウイルスバスター ビジネスセキュリティ

最新ステータス デバイス 検索 アップデート レポート 管理 ヘルプ ログオフ

デバイス > ポリシーの設定: デスクトップ (初期設定)

不正プログラム対策

検索方法

ウイルススキャン対策

機械学習型検索

挙動監視

信頼済みプログラム

隔離

WEB評価

Webレピュテーション

URLフィルタ

承認済み/ブロックするURL

その他の設定

ファイアウォール

オフィス内

オフィス外

単一IP

ホスト名:

名前解決

IPアドレス:

開始値

終了値

IP範囲 (IPv4またはIPv6)

プレフィックス:

長さ:

範囲: (IPv6)

保存 キャンセル

6 リストに追加されたことを確認します。

7 同様な手順で、必要な設定をすべて追加してください。追加が完了したら、[保存] をクリックします。

ウイルスバスター ビジネスセキュリティ

最新ステータス デバイス 検索 アップデート レポート 管理 ヘルプ ログオフ

デバイス > ポリシーの設定: デスクトップ (初期設定)

不正プログラム対策

検索方法

ウイルススキャン対策

機械学習型検索

挙動監視

信頼済みプログラム

隔離

WEB評価

Webレピュテーション

URLフィルタ

承認済み/ブロックするURL

その他の設定

ファイアウォール

オフィス内

オフィス外

デバイスコントロール

<input type="checkbox"/>	ID	名前	処理	方向	プロトコル	ポート/ポート範囲	コンピュータ
<input type="checkbox"/>	1	DNS	許可	送受信	TCP/UDP	指定: 53	すべて
<input type="checkbox"/>	2	NetBIOS	許可	送受信	TCP/UDP	指定: 137、...	すべて
<input type="checkbox"/>	3	HTTPS	許可	送受信	TCP	指定: 443	すべて
<input type="checkbox"/>	4	HTTP	許可	送受信	TCP	指定: 80	すべて
<input type="checkbox"/>	5	Telnet	許可	送受信	TCP	指定: 23	すべて
<input type="checkbox"/>	6	SMTP	許可	送受信	TCP	指定: 25	すべて
<input type="checkbox"/>	7	FTP	許可	送受信	TCP	指定: 21	すべて
<input type="checkbox"/>	8	POP3	許可	送受信	TCP	指定: 110	すべて
<input type="checkbox"/>	9	MSA	許可	送受信	TCP	指定: 16372、...	すべて
<input type="checkbox"/>	10	LDAP	許可	送受信	TCP/UDP	指定: 389	すべて
<input type="checkbox"/>	11	SNS-LAN	許可	送受信	UDP	指定: 5093	すべて

保存

手動検索 / 予約検索の除外設定

- 1 [検索] - [手動検索]、または[予約検索]をクリックします。
ここでは[手動検索]で記載しますが、[予約検索]も設定方法は同じです。

The screenshot shows the Trend Micro Virus Buster Business Security console. The top navigation bar includes '最新ステータス', 'デバイス', '検索', 'アップデート', 'レポート', '管理', and 'ヘルプ'. The '検索' menu is expanded, and '手動検索' is highlighted with a red box and a circled '1'. Below the navigation, a green checkmark indicates that the system is protected. The main content area displays 'セキュリティリスクの検出数' (Security Risk Detection Count) for the last 30 days, showing 0 for known threats, unknown threats, and policy violations. A table lists event types and their counts: ウイルス/不正プログラム (0), スパイウェア/グレーウェア (0), Webレピュテーション (0), and ネットワークウイルス (0). Other sections include 'ランサムウェアの概要' (Ransomware Overview) and 'エージェントのステータス' (Agent Status).

- 2 除外設定するコンピュータグループをクリックします。

The screenshot shows the '手動検索' (Manual Search) settings page. The page title is '検索 > 手動検索'. Below the title, there is a instruction: 'セキュリティ上の脅威を検索するグループを選択してください。検索設定を変更するには、グループ名をクリックして、新しい設定を保存します。' (Select the group to search for security threats. To change search settings, click the group name and save the new settings). A table lists the groups to be searched, with checkboxes for each. The 'サーバ (初期設定)' and 'デスクトップ (初期設定)' groups are selected, and this table is highlighted with a red box and a circled '2'. At the bottom, there are two buttons: '検索実行' (Execute Search) and '検索の停止' (Stop Search).

3 [検索除外] の [+] をクリックします。

The screenshot shows the Trend Micro Virus Buster Business Security interface. At the top, there is a navigation bar with tabs for '最新ステータス', 'デバイス', '検索', 'アップデート', 'レポート', '管理', and 'ヘルプ'. Below this, the main content area is titled '検索 > 手動検索 > デスクトップ (初期設定) : ウイルス/スパイウェア対策'. There are two tabs: '検索対象' and '処理'. Under '検索対象', there are three radio button options: '検索可能なすべてのファイル' (selected), 'トレンドマイクロの推奨設定: 実際のファイルタイプによる識別', and '検索対象の拡張子の選択'. Below these is a list of file extensions. There are also checkboxes for 'ネットワークドライブおよび共有フォルダを検索する' and '圧縮ファイルを検索する'. A dropdown menu for '最大レイヤ数' is set to '2'. At the bottom, there are two expandable sections: '検索除外' (highlighted with a red box and a circled '3') and '詳細設定'.

4 [検索除外を有効にする] がONであることを確認します。

5 弊社製品がインストールされているフォルダパス「C:¥FCAPP」を入力します。
(Cは弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。)
参照ツリーなどは表示されないため、手入力する必要があります。
指定したフォルダのサブフォルダも除外対象となります。

6 [追加] ボタンをクリックします。

The screenshot shows the '検索除外' dialog box in the Trend Micro Virus Buster Business Security interface. The dialog has a title bar 'TREND MICRO ウイルスバスター ビジネスセキュリティ' and a 'ログオフ' button. There are two sections: '特定ディレクトリの検索除外' and '特定ファイルの検索除外'. In the '特定ディレクトリの検索除外' section, there is a checked checkbox '検索除外を有効にする' (highlighted with a red box and a circled '4'). Below it, there is a checked checkbox 'トレンドマイクロ製品がインストールされているディレクトリを検索から除外する'. A text input field contains 'C:¥FCAPP' (highlighted with a red box and a circled '5'). To the right of the input field is a close button 'x' and an '追加' button (highlighted with a red box and a circled '6'). Below the input field is a '削除' button. In the '特定ファイルの検索除外' section, there is a text input field and an '追加' button.

7 下部のリストに、フォルダパスが追加されたことを確認します。

The screenshot shows the 'Exclusions' (検索除外) section of the Trend Micro Virus Buster Business Security interface. The 'Exclude search' (検索除外を有効にする) checkbox is checked. Under 'Exclude specific directories' (特定ディレクトリの検索除外), the checkbox 'Exclude Trend Micro products installed directories from search' (トレンドマイクロ製品がインストールされているディレクトリを検索から除外する) is also checked. Below this, there is a text input field containing 'C:%FCAPP', which is highlighted by a red box with a red circle containing the number 7. To the right of the input field are 'Add' (追加) and 'Delete' (削除) buttons. The 'Exclude specific files' (特定ファイルの検索除外) section is also visible below.

8 以下のフォルダーが存在する場合は、同様な手順で、それぞれリストに追加してください。
存在しない場合は追加不要です。

- ・32 ビットOS の場合「C:%Program Files %Common Files%Fukui Computer Shared」
- ・64 ビットOS の場合「C:%Program Files (x86)%Common Files%Fukui Computer Shared」

The screenshot shows the 'Exclusions' (検索除外) section of the Trend Micro Virus Buster Business Security interface. The 'Exclude search' (検索除外を有効にする) checkbox is checked. Under 'Exclude specific directories' (特定ディレクトリの検索除外), the checkbox 'Exclude Trend Micro products installed directories from search' (トレンドマイクロ製品がインストールされているディレクトリを検索から除外する) is also checked. Below this, there is a text input field containing two lines: 'C:%FCAPP' and 'C:%Program Files (x86)%Common Files%Fukui Computer Shared'. This input field is highlighted by a red box with a red circle containing the number 8. To the right of the input field are 'Add' (追加) and 'Delete' (削除) buttons. The 'Exclude specific files' (特定ファイルの検索除外) section is also visible below.

- 9 追加が終わったら、下にスクロールして [保存] をクリックします。
以上で終了です。

The screenshot shows the Trend Micro Virus Buster Business Security web interface. The top navigation bar includes the Trend Micro logo, the product name 'ウイルスバスター ビジネスセキュリティ', and a 'ログオフ' (Logout) button. Below this is a red navigation menu with options: '最新ステータス', 'デバイス', '検索', 'アップデート', 'レポート', '管理', and 'ヘルプ'. The main content area is titled 'デバイス > ポリシーの設定: デスクトップ (初期設定)'. On the left is a sidebar menu with categories like '不正プログラム対策', 'ウイルススabweア対策', '機械学習型検索', '挙動監視', '信頼済みプログラム', '隔離', 'WEB評価', 'Webレビューション', 'URLフィルタ', '承認済み/ブロックするURL', 'その他の設定', 'ファイアウォール', 'デバイスコントロール', 'ユーザツール', and 'エージェントの権限'. The main content area is titled '特定の拡張子を持つファイルの検索除外' (Exclusion of files with specific extensions) and contains a list of file extensions (XLSX, XLT, XLTM, XLTX, XML, Z, ZIP) in a scrollable box, an '追加' (Add) button, and a '削除' (Remove) button. To the right is a box labeled '選択された拡張子:' (Selected extensions) containing EVT, EVTX, LOG, OST, and PST. Below the extension list is a text input field for '拡張子を入力してください。' (Enter extension). At the bottom of the main content area, there is a '詳細設定' (Advanced Settings) link and a '保存' (Save) button, which is highlighted with a red box and a circled '9'.